NASA Procedural Requirements

COMPLIANCE IS MANDATORY

NPR 1600.1
Effective Date:
November 03, 2004
Expiration Date:
November 03, 2014

Printable Format (PDF)

Request Notification of Change (NASA Only)

Subject: NASA Security Program Procedural Requirements w/Change 2 (4/01/2009)

Responsible Office: Office of Protective Services

| TOC | ChangeHistory | Preface | Chapter1 | Chapter2 | Chapter3 | Chapter4 | Chapter5 | Chapter6 | Chapter7 | Chapter8 | Chapter9 | Chapter10 | AppendixA | AppendixB | AppendixC | AppendixD | AppendixE | AppendixF | AppendixG | AppendixH | AppendixI | AppendixJ | AppendixK | AppendixL | AppendixM | AppendixN | AppendixO | ALL |

Chapter 7: Physical Security Program

7.1 Security Control at NASA Centers

7.1.1. Each Center shall apply and maintain appropriate physical security measures necessary to provide for protection of persons and property.

7.1.2. Positive entry controls shall be implemented at all entry points to the Center and individually designated security areas and facilities, as deemed necessary, to preclude unauthorized access to critical areas, information, or personnel.

7.1.3. Procedures shall be established to ensure only authorized personnel are admitted to NASA Headquarters and field Centers.

7.2 NASA Photo-Identification (Photo-ID) Badge Program

7.2.1. NASA currently employs an Agency-specific employee photo-ID badge or Center-specific visitor pass to ensure only properly authorized personnel are granted access to NASA Centers, facilities, and other resources.

7.2.2. The CCS shall develop and monitor local procedures pertaining to the issuance, utilization, control, and accountability of the NASA Photo-ID badge and any Center-specific visitor passes.

7.2.2. NASA photo-ID badges are color-coded to designate the following categories of personnel, as specified in Appendix I, NASA Photo-Identification Standards. These photo-ID badges are required as official identification for entry to NASA facilities:

7.2.2.1. NASA civil service

7.2.2.2. NASA non-appropriated fund employees

7.2.2.3. Consultants/contractors

7.2.2.4. Other Federal agency employees and military personnel detailed to NASA

7.2.2.5. COOP students, summer students

7.2.2.6. Appropriately accredited members of the press

7.2.2.7. Foreign national visitors and contractor employees from designated and non-designated countries. Includes lawful permanent residents (LPR).

7.2.3. Security clearance status shall not be designated by any device, color, or code on any NASA photo-ID.

7.2.4. The NASA photo-ID issued to NASA civil service employees and other Federal agency and military detailees shall be honored for access to NASA Headquarters and all NASA Centers.

7.2.5. NASA photo-ID badge system databases shall be designated "sensitive unclassified information" and protected as ACI.

7.2.6. At a minimum, a favorable review; conducted by center security personnel, of submitted investigative documentation (e.g., SF 85, SF 85P, SF 86, NASA Form 531, etc.) is required for issuance of the NASA photo-ID to authorized NASA civil service, NASA contractor, and tenant organization personnel. See chapters 2, 3 & 4 for specific investigative requirements.

7.2.7. Issued NASA photo-ID badges or visitor passes shall be properly displayed and worn at all times while bearer is on a NASA Center or Component Facility. They shall be worn:

7.2.7.1. Above the waist on the outermost garment.

7.2.7.2. Photo-side visible.

7.2.8. The use of a permanent-type symbol or the affixing of any device (e.g., tenure pin, etc.) on the NASA photo-ID (or any alteration or modification thereof) is not authorized.

7.2.9. The NASA photo-ID is not personal property. It is the property of the U.S. Government. All personnel are responsible for appropriately safeguarding issued NASA photo-ID's; immediately reporting the loss or false use of a NASA photo-ID; challenging unbadged personnel; notifying the CCS of a name change; properly displaying the badge when on Center; and surrendering the NASA photo-ID upon resignation or retirement, or upon the direction of the issuing authority.

7.2.10. NASA Retiree ID Card. The Center HR Office shall initiate the request for the NASA Retiree ID Card only for those NASA Civil Service employees who have retired under favorable conditions (e.g., instances other than retired in lieu of termination for

cause, etc.). The issuance and use of the NASA Retiree Card is a privilege that may be denied or revoked at any time for cause.

7.2.10.1. The NASA Retiree photo-ID Card is valid at any NASA Center and when presented along with another appropriate form of photo-identification shall be used to obtain a visitor pass to enter the Center.

7.2.10.2. Access shall normally be restricted to business hours only, unless after hours access is "sponsored" and monitored by a Center employee.

7.2.10.3. All Center procedures and controls for visitor pass and visitor access, to include escorting, shall be observed as appropriate.

7.2.11. Forging, falsifying, or allowing misuse of a NASA Photo-ID or other forms of NASA identification in order to gain unauthorized access to NASA facilities is punishable under 18 U.S.C. 799 by fine or imprisonment for not more than 1 year, or both, and may further result in termination of employment and access to NASA facilities.

7.2.12. To deter duplication, falsification, and misuse, the NASA photo-ID shall be redesigned and reissued, at a minimum, every 6 years.

7.3 NASA Photo-ID Issuance Criteria

7.3.1. NASA Civil Service personnel photo-ID: NASA civil service personnel are issued Agency-unique color-coded photo-identification that clearly identifies the individual as a NASA employee. The NASA Photo-ID design, color, and other characteristics are established in Appendix J, NASA Photo Identification Card Standards.

7.3.1.1. Issuance of the NASA civil service personnel NASA photo-ID is restricted to U.S. Citizens only, with the following exception:

7.3.1.2. The NASA civil service personnel photo-ID may be issued to non-Federal employees (e.g., consultants, IPA's, Foreign Nationals) including foreign members of the Astronaut Corps, employed under an IPA when:

a. a. Such issuance is deemed to be in the best interest of the Agency.

b. b. The individual is nominated by a Center Director, in writing with sufficient justification for consideration and approval by the AA/OSPP.

7.3.1.3. As a reminder, when issued, the permanent NASA photo-ID provides an individual with official NASA civil service personnel identification resulting in the assumption on the part of NASA employees, Center management, and Center Security Officials, that they are dealing with a U.S. citizen. Therefore, care must be taken to:

a. Ensure these personnel are appropriately screened and restrictions imposed where appropriate to preclude inadvertent access to areas, meeting, conferences, and information (e.g., export controlled information, other forms of SBU, etc.) not authorized through the implementing hiring agreement.

b. Ensure appropriate notification, to all Center security offices when issuance of this photo-ID occurs so that restrictions outlined in subparagraph a above are implemented. .

7.3.1.4. As a reminder, when issued, the NASA photo-ID provides an individual with

official NASA civil service personnel identification; therefore, care must be taken to ensure appropriate awareness and due consideration of the risk involved.

7.3.2. Non-NASA Employee NASA Photo-ID. Contractor employees, consultant, military or other Government agency detailees, students, interns, and accredited press shall be issued a unique color-coded NASA photo-ID, per design specifications established in Appendix I. Dependent upon the type of access privileges authorized, the individually issued NASA photo-ID shall contain embedded (e.g., proximity chip) and exterior technology (e.g., bar code, magnetic strip) necessary to activate facility access control systems or to access IT resources as required to perform the individual's mission.

7.3.3. Foreign National (FN) NASA Photo-ID. All Foreign Nationals, except Astronauts, visiting or assigned to work at NASA Installations shall be issued a unique color-coded NASA photo-ID unless the exception established in subparagraph 7.3.1.2 above is granted. Dependent upon the type of access privileges authorized, the individually issued NASA photo-ID shall contain embedded (e.g., proximity chip) and exterior technology (e.g., bar code, magnetic strip) necessary to activate facility access control systems or to access IT resources as required to perform the individual's mission.

7.3.3.1. Specific and prominent lettering on the front of all FN NASA photo-ID will be placed identifying the bearer as a Foreign National and whether the FN is from a non-designated or designated country. This shall be accomplished with the placement of the letters "FN" for non-designated and "FND" for designated countries on the front of the NASA photo-ID.

7.3.3.2. An expiration date that is the earlier of the expiration of the individual's foreign passport, the expiration of the U.S. visa, or such earlier date as determined through review and approval pursuant to NPR 1371.2A, "Procedural Requirements for Processing Requests for Access to NASA Installations or Facilities by Foreign Nationals or U.S. citizens who are Representatives of Foreign Entities."

7.3.3.3. If the Foreign National is deemed to require an escort per chapter 4, section 4.13, the issued photo-ID shall be so labeled with the words "Escort Required" on the face of the badge, and procedures shall be developed to ensure the escort requirement is appropriately implemented and monitored to ensure compliance.

7.3.3.4. Access and movement restrictions, if any, shall be placed on the back of the FN NASA photo-ID and recorded on a Security/Technology Control plan as required in chapter 4, paragraph 4.13.9.

7.3.3.5. The term foreign national applies to all non-U.S. citizens.

7.3.4. Center Security Offices, in coordination with Center Chief Information Officers, will establish the procedures necessary to ensure the NASA photo-ID and necessary access privileges to controlled facilities and/or IT Systems are properly activated at the time of badge issuance. Procedures must include necessary guidance to facility managers and IT System owners for identifying and requesting activation of specific privileges.

7.4 NASA Photo-ID Color-Coding

7.4.1. Gold NASA Photo-ID - NASA civil service personnel, and all active members of the NASA Astronaut Corps. Accepted for access to all NASA Centers, as appropriate.

7.4.1.1. Foreign National members of the Astronaut Corps shall have a representation of

their National Flag superimposed on the badge for further designation as a FN.

7.4.2. Blue NASA Photo-ID - NASA consultants and contract employees (U.S. Citizen) who require access to a NASA Center or controlled facility.

7.4.3. Green NASA Photo-ID - Military and other U.S. Government agency detailees. Accepted for access to all NASA Centers, as appropriate.

7.4.4. Violet NASA Photo-ID - Any intern/student (U.S. citizen) who requires access to a NASA Center to perform their duties.

7.4.5. Orange NASA Photo-ID - Any foreign national (FN) contractor personnel from non-designated countries who require access to a NASA Center, or NASA controlled facility to perform their work.

7.4.6. Red NASA Photo-ID - Any Foreign National (FND) contractor personnel from designated countries who require access to NASA IT systems or shall have a need to work at a NASA controlled facility to perform their work.

7.4.7. Brown NASA Photo-ID - Any accredited member of the media (U.S. only) who may require access to "public" areas only of a NASA Center.

7.4.8. Silver NASA Photo-ID - Employees of the Jet Propulsion Laboratory (JPL).

7.4.9. If an individual does not require access to controlled Center assets, a local Center specific photo-ID may be issued in lieu of the NASA photo-ID.

7.4.10. Foreign national visitors shall be issued a visitor's pass, specifically identifying them as a foreign national, and escorted at all times.

7.5 Inspection of Persons and Property

7.5.1. General.

7.5.1.1. In the interest of national security and general employee safety, NASA shall provide appropriate and adequate protection or security for personnel, property, installations (including NASA Headquarters, Center, and Component Facilities), and information in its possession or custody.

7.5.1.2. In furtherance of this policy, NASA reserves the right to conduct an inspection of any person and property in their possession as a condition of admission to, or continued presences on, or upon exit from, any NASA Installation. Requirements, policy, and procedures for all aspects of this program are contained in 14 CFR part 1204, subpart 10.

7.5.1.3. All NASA entities must adhere to these requirements in the implementation of this program.

7.5.2. Requirements.

7.5.2.1. Per 14 CFR, Section 1204.1003 all entrances to Centers shall be conspicuously posted with the following notices:

1. " CONSENT TO INSPECTION: Your entry into, continued presence on, or exit from, this installation is contingent upon your consent to inspection of person and property.

2. UNAUTHORIZED INTRODUCTION OF WEAPONS OR DANGEROUS MATERIALS IS PROHIBITED: Unless specifically authorized by NASA, you shall not carry, transport, introduce, store, or use firearms or other dangerous weapons, explosives or other incendiary devices, or other dangerous instrument or material likely to produce substantial injury or damage to persons or property."

7.5.2.2. Only properly trained members of the Center's security organization shall conduct inspections pursuant to this NPR and the CFR. Personnel may be supplemented with detection devices (mirrors, x-ray, other sensing devices) and/or canines as the situation dictates.

7.5.2.3. Training shall include:

a. Appropriate search techniques for the type of vehicle being searched.

b. Key locations where devices or other contraband may be secreted.

c. Procedures for confiscating illegal or dangerous items, detaining of individuals and referring incidents to appropriate external law enforcement.

7.5.2.4. Such inspections shall be conducted in accordance with the following guidelines:

a. Consent to inspection notices covering NASA employees, contractors, and visitors to NASA Centers shall be issued in accordance with the authority contained under Section 304(a) of the National Aeronautics and Space Act of 1958, as amended, 42 U.S.C. 2455(a), and 14 CFR section 1204.1003.

b. A consent to the inspection must be obtained from the person to be inspected giving permission for a general exploratory inspection while that person is about to enter or is on the grounds of, or is about to depart from a NASA Center. The person may change their mind at any time, and inspection shall not be pursued further. If an individual does not consent to an inspection, it shall not be carried out, and the individual shall be denied admission to, or be escorted from, the Center.

c. Inspecting personnel must exercise good judgment at all times prior to or while conducting an inspection. They must avoid exceeding their authority or exercising their authority with undue severity.

d. Security personnel shall present appropriate NASA credentials to the subject of the inspection.

e. If, during inspection, an individual is found to be in unauthorized possession of items believed to represent a threat to the safety or security of the Center (e.g., weapons, drugs, explosives), the items may be confiscated, the individual shall be denied admission to, or be escorted from, the Center; or detained at the scene while the appropriate investigation is conducted by NASA investigators. The NASA Office of Inspector General or appropriate law enforcement authorities shall be notified to assume jurisdiction over the matter.

f. The Office of the General Counsel shall approve Agency procedures based upon the requirements of this section.

7.6 Security Areas

7.6.1. Types of Security Areas.

7.6.1.1. Restricted Area. An area in which security measures are taken to safeguard and control access to property and hazardous materials or to protect operations that are vital to the accomplishment of the mission assigned to a Center or Component Facility. All facilities designated as critical infrastructure or key resource shall be "Restricted" areas (as a minimum designation).

7.6.1.2. Limited Area. An area in which security measures are taken to safeguard classified material or unclassified property warranting special protection. To prevent unauthorized access to such property, visitors shall be escorted or other internal restrictions implemented, as determined by the CCS.

7.6.1.3. Closed Area. An area in which security measures are taken to safeguard classified material where entry to the area alone provides visible or audible access to classified material.

7.6.1.4. Temporary Secure Work Area (TSWA). An area in which security measures are needed for 30 days or less. Shall be of a "restricted," "limited," or "closed" nature. A TSWA shall also be established if approval as a permanent security area is pending.

7.6.2. Establishment, Maintenance, and Revocation.

7.6.2.1. Establishment. Center Directors; Director, Headquarters Operations; the AA/OSPP; and the CCS shall establish, maintain, and protect such areas designated as restricted, limited, or closed depending on the rationale for the establishment of the area and the area's vulnerability to unauthorized access.

7.6.2.2. Maintenance. Security measures shall vary according to individual situations; however, the following minimum-security measures shall be taken in all security areas:

a. Post appropriate signs at entrances and at intervals along the perimeter of the designated area, as appropriate for the facility, to provide reasonable notice to persons that the area is a security area.
b. Signs must read as shown in Appendix G; however, the AA/OSPP may approve existing signs now used pursuant to a State statute.
c. Regulate authorized personnel entry and movement within the area; deny entry to unauthorized persons or material.

7.6.2.3. Revocation. Once the need for a security area no longer exists, the area must return to normal procedures as soon as practical.

7.6.3. Access. Only those NASA employees, contractors, and visitors who need access and who meet the following criteria shall enter a security area unescorted. All other individuals must be escorted. Escorts must be authorized NASA employees or NASA contractors (U.S. Citizens).

7.6.3.1. To enter a Restricted Area unescorted, individuals must undergo the appropriate investigation required for that area as established by the individual Center; the investigation shall be, at a minimum, a NACI for civil service employees and a NAC for non-NASA personnel.

7.6.3.2. To enter a Limited Area, individuals must have a need-to-know and a security clearance equal to the classification of material in the area or, at a minimum, a NACI for unclassified but sensitive information and material.

7.6.3.3. To enter a Closed Area, individuals must have a need-to-know and a security clearance equal to the classification of the material in the area.

7.6.3.4. Center Directors and the AA/OSPP shall rescind previously granted authorizations to enter security areas when an individual's clearance and need-to-know is no longer justified, their presence threatens the security or safety of the property, or when access is no longer required for official purposes.

7.6.4. Cellular phones and other devices with digital camera capability. When introduced into security areas and/or areas of a sensitive nature, these items pose an unacceptable security risk to NASA. This risk encompasses numerous facets of the NASA security program. These risks include, but are not limited to: the protection of information (both classified and unclassified but sensitive (SBU) such as ACI and ITAR information); contract proceedings and information; investigative information; and employee right to privacy. The Center CCS will implement and enforce the following:

a. No cell phones or other devices with photographic capabilities may be introduced into a NASA area housing the processing, display, or open storage of classified information.
b. Each Center Security Office shall conduct a continuing review of their facilities to ascertain the locations of other sensitive functions requiring protection from an overt or inadvertent compromise utilizing such devices.
c. Centers must have written security plans to accomplish the protection of those areas. Copies of those plans shall be maintained in the Center Security Office, and a copy must be available within the protected area at all times. Plans must include, as a minimum, the following items:

1. The method used to alert and educate affected employees.
2. Details on how the policy shall be enforced, including how the devices shall be physically denied entry or otherwise controlled.
3. Spot-check procedures.

7.6.5. Two-way pagers and other communications devices capable of recording and sending text messaging are also not authorized in security risk areas.

7.7 Facility Security

7.7.1. NASA Buildings and Facilities.

7.7.1.1. NASA buildings and facilities come in varying types and sizes, are used for varying purposes, and require implementation of varying levels of security to ensure adequate protection of NASA personnel and assets.

7.7.1.2. Facilities and buildings shall be provided the level of security commensurate with the level of risk as determined by conducting a vulnerability risk assessment:

a. Physical security enhancements for existing facilities shall be established based on an assessment of the type of vulnerability(ies) identified during a security vulnerability risk assessment, development of strategies to address identified vulnerabilities, and implementation of selected security measures, both physical and procedural.

b. Minimum physical security requirements shall be incorporated into construction of facilities projects in accordance with the requirements established by the CCS, Facility Engineering, and the Interagency Security Committee (IASC).

c. Procedural security measures shall be developed, implemented, and properly disseminated to ensure awareness, adherence, and compatibility with implemented physical security measures.

7.7.2. Security Fencing.

7.7.2.1. When used properly and in conjunction with other physical and procedural security measures, fencing provides for a cost-effective method of delineating U.S. Government property boundaries, establishing clearly visible protected borders, and serving as a deterrent to most would-be intruders.

7.7.2.2. Selection and placement of security fencing shall be in accordance with the requirements established in Chapter 6, NPR 1620.3, Physical Security Requirements for NASA Facilities and Property.

7.7.3. Keys, Locks, Locking Devices (hasps and chains), and Protective Seals.

7.7.3.1. Despite the growth and sophistication of IT-based access control systems, traditional keys, locks, and seals continue to play a significant role in the implementation and management of facility and asset protection.

7.7.3.2. Center Security Officials shall establish key and lock control policies and procedures in accordance with Chapter 5, NPR 1620.3, Physical Security Standards for NASA Facilities and Property.

7.7.4. Minimum Protection Considerations for MEI Facilities or areas housing MEI assets.

7.7.4.1. A Facility Security Manager (FSM) shall be designated for each facility. The FSM shall ensure that security training is provided to employees with access to the MEI asset and that program management implements and enforces the security requirements developed for the asset.

7.7.4.2. An access control system shall be employed at all times.

7.7.4.3. Intrusion Detection Systems (IDS) and other surveillance systems (e.g., video surveillance), when required, shall be appropriately monitored and shall receive appropriate response by armed mobile security personnel capable of responding within locally established time limits, but shall not exceed 5 minutes. Unannounced response tests shall be performed at a minimum of twice in a calendar year. ,

7.7.4.4. Security fencing shall be installed when the need is identified during the conduct of security vulnerability risk assessments.

7.7.4.5. Security lighting shall be installed at key areas around the facility to facilitate, to the extent possible, detection of intruders.

7.7.4.6. All personnel requiring unescorted access to the MEI shall have been investigated per chapters 3 or 4. All personnel not meeting investigative requirements shall be escorted.

7.7.4.7. Personnel shall properly display issued photo-ID.

7.7.4.8. NASA MEI shall be designated and properly posted as a NASA "Restricted" area, at a minimum. See Section 7.6 for criteria regarding designation of NASA Security Areas.

7.7.4.9. After completion of an initial security vulnerability risk assessment upon designation as an MEI asset, reassessments shall be conducted every 2 years at a minimum, or more frequently as circumstances warrant.

7.7.5. Childcare Centers

7.7.5.1. Childcare centers established under the auspices of NASA sponsorship shall, with coordination and approval of the CCS:

a. Establish positive measures to ensure the proper identification of authorized personnel, to include parents and others, authorized to pick up children.
b. Establish physical and procedural security measures necessary to separate and control child areas from visitor reception areas.
c. Install duress system buttons at key locations per Security Office specifications.
d. Install video surveillance capability in key locations per Security Office specifications.
e. Ensure adequate mechanisms are in place for emergency notification and response.
f. Ensure appropriate security lighting is installed at key areas around the facility to enable detection of would-be intruders.

7.7.5.2. Minimum physical security and antiterrorism construction standards for new NASA Childcare Centers shall be incorporated into construction of facilities projects in accordance with the requirements established in NPR 8820.2E, NASA Facility Project Implementation Guide, and the Interagency Security Committee (IASC).

7.7.6. Visitor Centers and Outdoor Displays

7.7.6.1. NASA Visitor Center and outdoor displays traditionally house one-of-a-kind, irreplaceable items of historical significance.

7.7.6.2. Such items are generally considered invaluable because they are irreplaceable and must be considered sensitive property. They must be reasonably protected.

7.7.6.3. The degree of protection necessary must be determined locally and in partnership between the Visitor Center curator, CCS, and supporting facility engineers.

7.7.6.3. Visitor Center buildings and apertures providing access to the building must be modified or constructed so as to delay a determined intruder long enough for a security force to respond.

7.7.6.4. Interior and exterior security lighting shall be provided in all Visitor Center

buildings in which sensitive property is located.

7.7.6.5. Viewing surfaces of exhibit or display cases shall be constructed of materials resistant to breakage and must be securely fastened into frames or into the container.

7.7.6.6. Large items of historical property that are displayed outdoors in Visitor Center parks shall be anchored to prevent theft.

7.7.6.7. Pilferable component parts shall be secured to the display or removed at the close of each business day.

7.7.7. Minimum Strongroom Physical Security Standards.

7.7.7.1. While generally considered sufficient for their intended purpose, the use of strongrooms to protect CNSI must be kept to the absolute minimum.

7.7.7.2. Any room designated for use as a strongroom must be modified in accordance with the following:

a. Doors shall be solid core metal clad and installed with the appropriate "X" Series tumbler lock.
b. Doors frames shall be steel.
c. Construction shall be a minimum of true floor to ceiling wood stud framing covered by 3/4" plywood and 1/2" wallboard. If necessary, plywood and new wallboard shall be installed directly over existing framing and wallboard.
d. Use of Intrusion Detection Systems (IDS) shall be determined by the CCS on a case-by-case basis and shall be evaluated on the basis of existing threats, overall building security program, and establishment of periodic security checks of facility.

7.7.8. IDS, Video Surveillance, and Electronic Access Control System Minimum Standards and Integration.

7.7.8.1. Security systems intended to protect people, property, or information are the responsibility of the CCS.

7.7.8.2. IDS, Video Surveillance, and Electronic Access Systems provide an effective means to enhance any organization's physical security program. If employed correctly and managed appropriately, these systems offer a wide range of coverage options.

7.7.8.3. The CCS shall:

a. Determine, in coordination with facilities engineering personnel with the appropriate expertise in security systems design, integration, and operation overall performance requirements for IDS, video surveillance, and Electronic Access Control Systems.
b. Establish and operate a 24-hour monitoring site where emergency response can be dispatched upon need.

7.7.8.4. Individual, stand alone systems offering no centralized monitoring oversight and alarm response capability (including internally-monitored systems) are not authorized.

7.7.9. For those facilities protected under the National Preservation Act of 1966,

implementation of security measures shall be those measures allowable under the Act, to the extent necessary and practical.

7.8 Airfield and Aircraft Security

7.8.1. The cost and criticality of aircraft assets require protection at the home port, at intermediate landing locations, and at destinations. The CCS, in concert with Center Airfield Operations Management personnel, shall:

7.8.1.1. Ensure that a physical security survey and security vulnerability risk assessment are conducted on resident aircraft, hangars, ramps, and airfields.

a. The security vulnerability risk assessment shall help to determine the level of criticality and vulnerability of NASA flight assets to theft, sabotage, terrorism, vandalism, and air piracy.

b. The survey shall be used to establish a requisite level of protection that is reasonable and sustainable.

7.8.1.2. Ensure that specific physical and procedural security measures for the protection of NASA aircraft, are implemented, as appropriate.

7.8.1.3. At a minimum, designate and post airfield and associated support facilities as "Restricted Areas," and establish appropriate access control measures.

7.8.1.4. With the assistance of aircraft commanders, develop physical security requirements tailored to the configuration of specific aircraft to be included in the Pilot's Aircraft Checklist.

7.8.1.5. Develop a procedure for reporting and responding to the unauthorized movement or taxiing of aircraft.

7.8.1.6. Develop an alerting system that promptly advises the tower, fire department, security force, and other appropriate authorities of unauthorized activity.

7.8.1.7. Develop a response procedure in the event of the unauthorized movement of an aircraft.

7.8.2. Aircraft Commanders shall:

7.8.1.1. Ensure security of their aircraft at transient domestic and international locations.

7.8.1.2. Prohibit unauthorized access to aircraft under NASA control.

7.8.1.3. Ensure that passengers are properly identified and that baggage and packages are either associated with passengers or are authorized NASA cargo.

7.8.1.4. Reject unaccompanied or unidentifiable luggage or cargo and release to the custody of Center or other Airfield security forces for appropriate disposition.

7.8.1.5. Conduct appropriate security inspections of any NASA aircraft before placing it in service and after it has been left unattended.

7.9 Control and Issuance of Arms, Ammunition, & Explosives (AA&E)

7.9.1. Authority.

7.9.1.1. The AA/OSPP shall direct or grant approval for the following security officers and employees to carry firearms on official duty:

a. The DSMD and designated HQ security personnel.

b. The CCS of each Center and designated security personnel.

c. NASA employees, contractors, and subcontractors, while engaged in the performance of their official security duties such as couriers, investigators, or protective operations and details. This does not include the OIG, whose authority is derived from other sources.

d. NASA contractors and subcontractors engaged in the protection of property owned by the United States and located on NASA Centers or component facilities.

7.9.2. Responsibilities.

7.9.2.1. NASA certifying officials, described in Chapter 10, "Glossary of Terms, Abbreviations, and Acronyms," shall ensure compliance with the requirements of this section.

7.9.2.2. NASA employees and contractors to whom firearms are issued are responsible for strict compliance with all the conditions regarding the carrying and use of firearms as established herein and set forth at 14 CFR part 1203b, Security Programs, Arrest Authority and Use of Force by NASA Security Force Personnel.

7.9.2.3. NASA security personnel and contractors shall not carry firearms outside the 50 States, the District of Columbia , and U.S. territories (Puerto Rico, Guam , U.S. Virgin Islands, American Samoa , et al.) without the advance approval of the AA/OSPP.

7.9.3. Certification to Carry Firearms.

7.9.3.1. The certifying official shall issue a NASA Form 699A or 699B, Certificate of Authority to Carry Firearms. The following items define the forms and their use and procedures for certification:

a. NASA Form 699A is a certification to carry concealed firearms when necessary in the performance of official duties.

b. The form shall be issued to NASA Civil Service employees and select contractor security officers (requires AA/OSPP approval) only. Uniformed contractor personnel shall not carry concealed weapons.

c. The NASA Form 699A is prepared in triplicate and indicates an expiration date (not to exceed 2 years from date of issue).

d. Upon termination of employment or assignment to duties not requiring carrying concealed weapons in the course of official duties, the certificate must be returned to the issuing officer within 15 days.

e. Exceptions to these requirements shall be made (in writing) only by the DSMD.

7.9.3.2. NASA Form 699B is a certification to carry unconcealed firearms that shall be issued only to NASA contractor employees serving as uniformed guards.

a. This form shall be prepared in duplicate and shall indicate the date of expiration (not to exceed the term of any applicable guard service contract; otherwise, not to exceed 5 years).

b. The form shall also identify the specific nature and location of official duties that require the carrying of firearms.

c. The original certificates shall be issued to the employee and shall be retained in the employee's possession while on official duty.

d. One copy of the certificate shall be retained by the NASA certifying official.

e. All losses of certificates shall be reported immediately to the certifying official.

f. Upon termination of employment or assignment to duty no longer needing certification to carry firearms, the original certificate shall be returned to the certifying official.

g. Only the certifying official may make exceptions to these requirements.

7.9.3.3. NASA Forms 699A and 699B are serialized for control and accountability purposes. Certifying officials shall maintain appropriate accountability records, including certification of destruction, for all forms in their custody and ensure that all unused forms are kept in a secure storage container other than the one in which the accountability records are stored.

7.9.3.4. Certifying officials shall not sign their own certificates. The Center Director or the AA/OSPP shall sign certificates authorizing the issue of a weapon to a certifying official.

7.9.4. Conditions Under Which Firearms May be Carried by Center Security Personnel. Including shoulder-fired weapons (e.g., rifles, machine guns, shotguns):

7.9.4.1. Firearms may be carried only when all of the following criteria are met:

a. The individual has successfully completed the appropriate suitability background investigation and has been favorably evaluated by a qualified physician to be physically fit as well as emotionally stable.

b. The individual is in immediate physical possession of a valid NASA certification to carry firearms.

c. The individual has successfully completed a qualification course for the firearm being carried, and the qualification is current. (Refer to Appendix E and paragraph 7.9.8)

d. It is necessary in the performance of official NASA duties and with the knowledge and approval of a certifying official.

e. There is no use of intoxicants (e.g., illegal drugs, alcohol) during duty and prior to 12 hours of reporting to duty.

f. Appropriate annual criminal hsitory check for recertification under the Lautenberg Amendment to the Gun Control Act of 1968, effective 30 September 1996.

7.9.4.2. The wide range of circumstances under which it shall be necessary to carry firearms requires consideration of all pertinent factors, augmented by common sense and good judgment.

7.9.5. Conditions Under Which Firearms and Explosives May be Used, Stored, and

Maintained by Non-Security Personnel:

7.9.5.1. Researchers and scientists frequently use firearms and explosives during testing and experimentation. The safe operation, storage, and accountability of firearms and explosives used under testing and experimentation are required to ensure the safety and security of Center personnel.

a. NASA Safety Manual and NASA Safety Standards (NSS) 1740.12, Safety Standards for Explosives, Propellants, and Pyrotechnics, are the governing documents for establishing the safe storage and handling of firearms and explosives.

b. This chapter is the governing document for issue, use, secure storage, and accountability for firearms and explosives.

7.9.5.2. The following procedures are required for the use, storage, and accountability of firearms and explosives by non-security personnel.

a. NASA program and project personnel contemplating the of use firearms or explosives in testing or experimentation programs must submit a written request to the CCS outlining the program or project need for introducing firearms, ammunition, and explosives onto a NASA facility.

b. An inventory of the type of weapons and explosives with serial numbers, type and amount of ammunition, and type and amount of explosives shall be maintained and updated on a quarterly basis. The inventory shall be made available for review by security and safety personnel, as requested.

c. Identify location of stored/secured and names of personnel having access.

d. In coordination with the Center Security and Safety personnel, establish appropriate secure storage for AA&E.

7.9.6. Weapons Aboard Commercial Aircraft.

7.9.6.1. Armed NASA Special Agents (SA) may only carry firearms on commercial aircraft after completion of required Federal Aviation Administration certification in accordance with 14 CFR 108.219, and then only in conjunction with "Official" Government travel requiring the SA to be armed.

a. Refresher Federal Aviation Administration certification training, for carrying firearms on a commercial aircraft, shall be required every 2 years and shall be integrated with required firearms qualification to ensure appropriate awareness.

b. The DSMD or designee shall be notified in advance of all official air travel of armed NASA Civil Service SA. NASA security services contractor personnel are not authorized to fly armed.

7.9.6.2. In addition to the Federal Aviation Administration requirement, the SA must be currently qualified to carry a firearm.

7.9.6.3. The SA must be in possession of a current NASA Form 699A (concealed weapons permit) and NASA badge and credentials.

7.9.6.4. The SA shall not display his/her weapon or make known to passengers that he/she is carrying a weapon.

7.9.6.5. The SA shall always carry the weapon on his/her person and never in carry-on

baggage.

7.9.6.6. The SA shall always carry handcuffs.

7.9.6.7. The SA shall never carry Oleoresin Capsicum spray or other chemical intermediate weapon while on-board a commercial flight.

7.9.7. Firearms Instruction.

7.9.7.1. The certifying official shall designate a firearms instructor, who shall inform the certifying official in writing of an individual's knowledge of the rules of firearm safety and the content of this NPR.

7.9.7.2. In cases involving a contractor guard force, the firearms instructor may be appointed from the guard force complement.

7.9.7.3. Minimum standards shall be met before a firearms instructor or certifying official shall consider an individual qualified to carry firearms.

7.9.7.4. Recent firearms training and experience during prior employment, such as the FBI, Secret Service, police, military, or other significant and qualifying experience, shall meet NASA standards if the individual has qualified under all provisions of this chapter within the past 30 days.

7.9.7.5. These qualifications shall be verified by a review of employment and training history either through an interview with previous management or visual inspection of documented training history.

7.9.7.6. Appropriate NASA training, including firearm safety procedures and use of deadly force, followed by obtaining a qualifying score on a recognized course as specified in paragraph 7.9.8 below, shall also be required.

7.9.8. Training.

7.9.8.1. Personnel shall be trained and qualified on professional firearm ranges established and maintained by NASA, or other federal, state, or municipal authorities.

7.9.8.2. Personnel shall be certified for carrying firearms after firing a qualifying score under the NASA certified firearm course. (See Appendix E of this NPR.)

7.9.8.3. The AA/OSPP shall establish firearms course of fire standards for all Center armed security personnel, to include standards for shoulder-fired weapons (e.g., rifles, submachine guns, shotguns).

7.9.8.4. As soon as possible after certification, personnel shall receive testing and training in judgmental shooting (whether to shoot or not to shoot) through NASA's current firearms training simulator or other approved methods of judgmental shooting.

7.9.9. Maintenance of Proficiency.

7.9.9.1. Personnel authorized to carry firearms shall be required to fire a qualifying score on the NASA course of fire at least once every 6 months.

7.9.9.2. All personnel authorized to carry firearms must successfully complete testing and training on the simulator or other approved methods of judgmental shooting annually, if possible, or as often as the system is available at that Center.

7.9.10. Records.

7.9.10.1. The certifying official or firearms instructor shall maintain records of personnel certified to carry firearms, including the basis for qualification, qualifying scores, rounds fired, and all other pertinent data.

7.9.10.2. Records shall be maintained for 2 years.

7.9.11. Firearms Standards.

7.9.11.1. CCS shall utilize only firearms listed in the NASA Approved Firearms List (AFL) to arm their Civil Service and contractor security staff.

7.9.11.2. The AFL is approved by the Office of Security and Program Protection (OSPP) and maintained by the NASA Federal Arrest Authority Training Academy (NFAATA) at Kennedy Space Center .

7.9.11.3. The AFL may be waived or modified only by the AA/OSPP.

7.9.11.4. Training, qualifications, and certification for all approved firearms shall be documented per paragraph 7.9.8.

7.9.11.5. Modifications.

a. No modifications to the operating system, firing mechanism, and/or trigger groups shall be made to any NASA approved firearms.

b. Center armorers shall modify grips, sights, and control levers to best suit individual users.

7.9.11.6. Handguns.

a. NASA approved handguns are semi-automatic pistols in calibers 9mm, .40, or .357.

b. Uniformed contractors at each Center must be armed with the same make and model handgun.

c. Emergency response teams/SWAT teams may carry a different make and model.

d. NASA Civil Service personnel shall carry the same make but may vary the model to suit individual users.

e. Handguns must always be worn in standard, commercially available holsters; uniformed officers must use holsters with a retention device.

7.9.11.7. Patrol Rifles.

a. At the discretion of the CCS, contractors shall be armed with semi-automatic or select fire patrol rifles.

b. Only iron or optical sights shall be installed on these weapons.

7.9.11.8. Patrol Shotguns.

a. At the discretion of the CCS, contractors and Civil Service personnel shall be armed with semi-automatic or pump action 12 gauge shotguns.

b. These weapons shall also be used to employ "less-lethal" ammunition.

7.9.11.9. Submachine guns.

At the discretion of the CCS, contractor security force may be armed with submachine guns.

7.9.12. Other approved firearms.

At the discretion of the CCS, and with the consent of the AA/OSPP, other firearms may be utilized to meet Center security requirements.

7.9.13. The user of any NASA approved firearm must meet the training and certification requirements of paragraph 7.9.8.

7.9.14. Personal weapons.

The use or carrying of personal weapons is prohibited.

7.9.15. Ammunition.

7.9.15.1. Only premium, commercially manufactured, "law enforcement only" duty ammunition shall be issued.

7.9.15.2. Duty ammunition shall be expended at training sessions at least once every 18 months to ensure use of fresh duty ammunition.

7.9.15.3. Normal training ammunition shall be commercially manufactured "lead-free" training ammunition designed for range use.

7.9.16. Firearm maintenance.

7.9.16.1. All firearms shall be periodically inspected and kept in good working order by a qualified gunsmith/armorer.

7.9.16.2. Ammunition, holsters, and related equipment shall be periodically inspected for deterioration and kept in good working order.

7.9.17. Accountability of Arms, Ammunition, and Explosives (AA&E).

7.9.17.1. The control and custody of all AA&E within a Center shall be under strict accountability at all times and is the ultimate responsibility of the CCS.

7.9.17.2. The CCS shall appoint a custodian for all AA&E within the Center Security Office, within each contractor guard force, and within each non-security organization using AA&E (e.g., explosives, propellants, etc.) for research or testing purposes.

7.9.17.3. Each custodian shall maintain an ongoing inventory of all AA&E. The inventory shall indicate:

a. The date and method of acquisition of all firearms and ammunition.

b. Full identifying data, e.g., the caliber, make, and serial number of each firearm.

c. Amounts of basic load and training ammunition on-hand.

d. Types and amounts of explosives, (e.g., fragmentary, flash-bang grenades, C/S, pepper spray, etc.).

7.9.17.4. The CCS shall report all Center AA&E data to the AA/OSPP on an annual basis the third week after the end of the fourth quarter of each fiscal year.

7.9.17.5. Current contractor firearm data shall be maintained in the Center Security Office.

7.9.17.6. A receipt system for recording the issuance, transfer, and return of all firearms, ammunition, and explosives, shall be maintained by the custodian. Receipts shall include the following details:

a. Dates of issuance, transfer, or return to custody.

b. Serial numbers of firearms.

c. Numbers and types of assigned explosives.

d. Types and numbers of ammunition on-hand.

e. Signatures of recipients.

f. Signatures of custodians upon return of the firearms and explosives.

(NOTE: Both NASA personnel and contractor receipts shall be retained by each Center for 1 year.)

7.9.18. Lost, stolen, or missing AA&E shall be reported immediately, but no later than 24 hours after discovery, to the DSMD:

a. This preliminary report shall include all available details concerning the event with a complete description of the weapon or other lost AA&E item(s).

b. This preliminary report shall not be delayed pending a complete report of the circumstances.

c. A description of the lost, stolen, or missing AA&E shall also be entered into the National Criminal Information Center (NCIC) database.

7.9.19. Security Services contract personnel issued AA&E may only be armed on NASA property to perform their mission, if approved by the CCS.

7.9.20. Non-security personnel having NASA mission related uses for AA&E items (e.g., researcher, scientists, etc.) shall:

7.9.20.1. Ensure control, storage and accountability of authorized AA&E are in accordance with the provisions in paragraph 7.9.21 of this chapter and the requirements established in the NASA Safety Manual and NASA Safety Standards (NSS) 1740.12, Safety Standards for Explosives, Propellants, and Pyrotechnics.

7.9.20.2. Maintain appropriate and current inventories of issued and maintained AA&E per paragraph 7.9.17 and provide a copy of the inventories to the CCS as changes occur.

7.9.21. Storage and Exchange of AA&E.

7.9.21.1. Issued firearms for NAS security and law enforcement personnel may be stored loaded or unloaded under secure means, per local policy.

7.9.21.2. When not in use, all issued firearms and ammunition shall be securely stored per local policy.

a. Non-issued firearms and shoulder-fired weapons shall be stored in an arms room or a security container with a built-in 3-position combination lock and issued only as required.

b. Non-issued ammunition shall be stored in either a suitable lockable container or an arms room.

7.9.21.3. Explosives shall be stored in separate secure containers, specifically designed for the purpose of storing explosive materials.

7.9.21.4. Firearms or ammunition shall not be stored in containers with money, drugs, precious materials, evidence, or CNSI. They shall be stored separately.

7.9.21.5. NASA HQ and each Center shall adopt procedures for the maintenance of records with respect to the issuance of AA&E and access to firearms and ammunition storage areas and containers.

7.9.21.6. Weapons shall not be exchanged on a guard post. Any exchange or inspection of firearms shall be done only in an area where a "clearing barrel" is available and under proper supervision.

7.9.21.7. Firearms shall always be considered loaded. Armed NASA security personnel shall not point the firearm at anything that they do not intend to shoot.

7.10 Standards for Secure Conference Rooms

7.10.1. When established as permanent facilities, NASA Secure Conference Rooms shall meet security standards outlined in DCID 6/9, "Physical Security Standards for Sensitive Compartmented Information Facilities."

7.10.2. The following measures shall be taken when infrequent classified meetings are held in rooms not configured in accordance with DCID 6/9.

7.10.2.1. Meetings shall be limited to collateral Secret or below.

7.10.2.2. Positive access control shall be implemented.

7.10.2.3. A Technical Surveillance Countermeasures (TSCM) Specialist, if available, or Security Officer shall conduct a visual inspection and establish security procedures for the meeting.

7.10.3. Special Cases.

7.10.3.1. The preceding specifications do not apply to conference areas in which the level of security exceeds the collateral Secret level.

7.10.3.2. For these areas, guidance on additional requirements will be provided by the CCS on a case-by-case basis.

7.10.3.3. The DSMD or CCS shall be contacted for any interpretation of these specifications.

7.11 Threat Assessment

7.11.1. Reliability.

7.11.1.1. NASA personnel, facilities, and programs are subject to a wide range of internal

and external threats.

7.11.1.2. Such threats may be presented by natural forces, workplace violence, the technological sophistication of NASA Research and Development (R&D) and test facilities and programs, and the inherent risk of component and system failure by both internal and external attempts to disrupt Agency operations or to compromise National security.

7.11.2. Threat Assessments.

7.11.2.1. The DSMD, after consultation and input from various sources, shall publish an annual NASA Postulated Threat Statement.

7.11.2.2. Of significant importance are the Agency's resources identified under the Critical infrastructure and key resources protection program. However, threat assessments must transcend formally designated critical resources and assets and cover the full realm of NASA personnel and physical resources, assets, and program/project information.

7.11.2.3. The CCS shall use the NASA Threat Statement in developing a localized threat statement for their Center.

7.11.3. Countermeasures.

7.11.3.1. NASA shall employ a sound and comprehensive security program that includes security awareness training and the development and implementation of Center security plans to counter these threats.

7.11.3.2. To ensure an Agencywide standard for reacting to periods of increased security threats, the threat conditions established in section 7.17 below shall be employed as directed by NASA Headquarters or as determined by local events.

7.12 Threat and Incident Reporting

7.12.1. General.

7.12.1.1. All Centers shall implement a threat and incident reporting system as required by NPD 1600.2, NASA Security Policy.

7.12.1.2. The system's purpose is to keep the Administrator and senior management officials advised on a timely basis of serious security-related incidents or threats that may affect the NASA mission.

7.12.1.3. Reports shall be forwarded to the DSMD. Refer to appendix F for a sample of the Serious Incident Report format.

7.12.2. Responsibilities.

7.12.2.1. The CCS ensures that incidents are reported to the DSMD and followed up with a fax that describes the incident.

7.12.2.2. The DSMD shall report information from the CCS (or designated representative) to the AA/OSPP, if available.

7.12.2.3. The AA for Security and Program Protection shall then decide whether it is appropriate to brief either the NASA Administrator, Deputy Administrator, or Chief of

Staff.

7.12.2.4. If a principal or designated representative is unavailable at any of the cited levels, the information shall be automatically passed to the next level.

7.13 Reportable Incidents

7.13.1. Any type of incident that might have security implications shall be reported to the AA/OSPP in a timely manner, including the following:

7.13.1.1. All crimes committed at a Center requiring notification of NASA OIG, or, as appropriate, the FBI, DEA, ATF, or local law enforcement.

7.13.1.2. Possible Espionage (Reported through Center CI channels via the NASA Secure Network (NSN)).

7.13.1.3. Possible Sabotage (Reported through Center CI channels via the NSN).

7.13.1.4. Suspected terrorist activity (e.g. surveillance, photography, attempted penetrations, unusual requests for information). (Reported through Center CI channels via the NSN).

7.13.1.5. Bombing incidents, including bomb threats that severely impact Center activities.

7.13.1.6. Actual or planned demonstrations or strikes.

7.13.1.7. Shootings or other violent acts.

7.13.1.8. All incidents which involve the need for professional medical attention or damage to NASA facilities or equipment exceeding $25,000 shall also be reported in accordance with NPR 8621.1, NASA Procedural Requirements for Mishap Reporting, Investigating, and Record Keeping.

7.13.1.9. All incidents occurring on NASA property that result in the death of a person. (NOTE: Deaths on NASA property may also require reporting to and through the NASA Safety Program channels in accordance with NPR 8621.1.)

7.13.1.10. A security-related incident in which the media has become involved and publicity is anticipated.

7.13.1.11. An adverse event in an automated systems environment that would be of concern to NASA management due to a potential for public interest, embarrassment, or occurrence at other NASA facilities. These incidents shall include unauthorized access, theft, interruption of computer/network services or protective controls, damage, disaster, or discovery of a new vulnerability.

7.13.1.12. Threats against NASA property.

7.13.1.13. Threats that affect NASA missions.

7.13.1.14. Threats against NASA personnel.

7.13.1.15. Information pertaining to the ownership or concealment by individuals or groups of caches of firearms, explosives, or other implements of war when it is believed that their intended use is for other than legal purposes.

7.13.1.16. Information concerning individuals who are perceived to be acting irrationally in their efforts to make personal contact with high Government officials; information concerning anti-American or anti-U.S. Government demonstrations abroad; information concerning anti-American and anti-U.S. Government demonstrations in the United States, involving serious bodily injury or destruction of property; or an attempt or credible threat to commit such acts to further political, social, or economic goals through intimidating and coercive tactics.

7.14 NASA Security Office Special Agent Badges and Credentials (B&C)

7.14.1. Control.

B&C's are sequentially numbered and accountable security items. Their issue, use, and accountability shall be monitored by both the AA/OSPP and the CCS.

7.14.2. Issuance, Use, and Return.

7.14.2.1. B&C's identify NASA Special Agents authorized, under NASA Federal Arrest Authority, to conduct investigations and inspections and to perform other duties that shall be assigned by virtue of the National Aeronautics and Space Act of 1958, as amended. [NOTE: This does not include the Office of Inspector General (OIG), whose authority is derived from other legal sources].

7.14.2.2. The AA/OSPP shall create, authenticate, and issue credentials and procure metallic badges at the request of the CCS.

7.14.2.3. The CCS shall nominate civil service personnel to receive B&C's.

7.14.2.4. Security specialists whose official duties do not require routine investigative work and/or frequent liaison with Federal, State, or local law enforcement authorities shall only be issued credentials appropriate for the position occupied.

7.14.2.5. The CCS shall ensure that B&C's or credentials no longer required for official duties are returned to the AA/OSPP. B&C's shall be surrendered to the CCS when replacements are issued.

7.14.2.6. The CCS shall ensure that B&C's are not misused and shall withdraw them immediately upon any report of misuse, pending investigation of the allegation:

a. A report outlining the circumstances of any withdrawal of B&C's shall be forwarded to the DSMD within 72 hours.

b. A report on the final disposition of the incident, including the results of a Return To Duty (RTD) assessment and recommendation, shall also be furnished to the DSMD for review and final determination.

7.14.2.7. Lost or stolen B&C's must be reported immediately. The appropriate CCS shall forward a report outlining all pertinent facts to the DSMD no later than 2 days after the loss.

7.14.2.8. Security specialists must surrender B&C's when requested by the issuing authority or when relieved of security duties by transfer, termination, or retirement. Upon termination of security duties, requests to keep B&C's shall be addressed as follows:

a. Employee must have been employed by NASA as a Security Official for a minimum of 10 years.

b. Credentials shall be sent, along with a letter requesting retention of "voided" credential, for the individual concerned.

c. Retirement and presentation of the NASA metal badge shall be considered based on the following prerequisites:

(1) Employee must be retiring from Federal service under honorable circumstances.

(2) Employee must have served NASA in an agent capacity for a minimum of 10 years.

(3) Badges must be mounted in a Lucite award block, which shall be funded by the either the individual or requesting office and procured by the OSPP.

(a) Individuals or organizations shall submit to the OSPP a written request containing the individuals name, position, and length of service with NASA, along with a personal check in the amount required at that time, made out to the OSPP selected vendor.

(b) The OSPP shall arrange fabrication of the award. Delivery time shall normally be within 4 weeks from submission of order.

7.14.2.9. B&C's may be returned to the AA/OSPP by NASA Pouch Mail, double wrapped, or they may be hand-carried.

7.14.3. B&C's for Contractors.

a. The CCS shall issue Center-unique B&C's to contractor security personnel as deemed appropriate. The B&C must identify the individual as a NASA Contract employee, authorized under the Space Act to perform specified duties (e.g., investigations, inspections, etc.).

b. All provisions of section 7.14 also apply to NASA contract security services personnel.

7.14.4. Acceptance of B&C's for Access to NASA Centers.

B & C's (Federal, State, or NASA) shall not be accepted for access to NASA Centers unless accompanied by a NASA photo-ID or issued NASA visitors pass.

7.15 Technical Surveillance Countermeasures (TSCM)

7.15.1. TSCM Program.

The AA/OSPP is responsible for the NASA TSCM program. The program shall be consistent with national policy issued by the U.S. Security Policy Board (USSPB). All matters pertaining to the conduct of TSCM activities throughout the Agency shall be directed and coordinated through the DSMD.

7.15.1.1. The AA/OSPP shall ensure that a NASA TSCM capability exists which can:

a. Conduct physical, electronic, and visual search techniques to identify and protect Agency persons, facilities, information, or activities that are vulnerable, through design or circumstance, to hostile technical surveillance activities.

b. Ensure that TSCM operations are conducted in a manner consistent with U.S. Security Policy Board guidelines.

c. Acquire and employ TSCM technologies, techniques, and methods to identify and neutralize hostile technical surveillance activities that are consistent with accepted national TSCM policies.

d. Collect, analyze, and disseminate data regarding the technical surveillance threat to the Agency.

e. Provide support by ensuring that all NASA TSCM personnel are accredited through U.S. Government TSCM training and that individuals receive continuing, advanced training necessary to maintain the level of technical expertise as prescribed by TSCM USSPB Procedural Guides 1 through 3.

f. Develop, with input by the DSMD; Director, Safeguards Division; and Center Security Chiefs, a listing of facilities that require a TSCM service.

g. Coordinate TSCM efforts with Centers that have organic TSCM assets.

7.15.1.2 Conduct of TSCM Services

a. TSCM services shall be conducted in accordance with USSPB TSCM Procedural Guides, following the four distinct phases.

b. TSCM services shall be coordinated through the DSMD for the purpose of tracking TSCM efforts.

7.15.1.3 Facilities Requiring TSCM Support

a. A TSCM service shall be performed for initial accreditation purposes for any Sensitive Compartmented Information Facility (SCIF) within the Agency. Follow-on TSCM support shall be coordinated through the Agency SSO when threat conditions warrant, when there has been a modification to the SCIF, when uncleared personnel have not been continually escorted while in the SCIF, or when new equipment or furnishing have been introduced to the SCIF.

b. A TSCM service shall be conducted in all offices in which Top Secret discussions routinely occur.

c. A TSCM service shall be conducted in offices or areas that are routinely used to process information or to discuss information that addresses sensitive aspects of controlled U.S. technology or controlled Agency technology.

d. TSCM services shall be conducted in NASA senior executive office spaces.

e. TSCM services shall be conducted in contractor facilities that process and discuss NASA classified national security information as annotated in the DD-254, DOD Contract Security Classification Specification.

f. TSCM in-conference monitoring support shall be scheduled if the conference is conducted in an area not usually associated with classified discussions and the area has not been under continuous control by cleared employees.

7.15.1.4 TSCM Request Procedures

All requests for TSCM support shall be addressed in writing to the DMSO, Security Management Division and classified at the Secret level at a minimum. Advanced coordination may be done telephonically, but only via secure means. When requesting

or coordinating a TSCM service, requestors shall not use any communication medium located within the area that is to be the subject of the TSCM service. At a minimum, the request must identify:

a. Complete identification of the area requiring TSCM support, to include: name of area, room number, building number, address, location, and brief mission description of the area/facility.

b. Brief justification why a TSCM service is necessary.

c. Square footage of each space identified.

d. The name of the point of contact and an alternate, with telephone numbers for both secure and nonsecure telephones.

e. Clearance requirements for TSCM personnel.

f. The time frame the service is required.

7.15.1.5 TSCM Reports

1. Upon completion of a TSCM survey, a complete report shall be provided for the requestor. At a minimum the report shall include:

a. Complete identification of the facility receiving the TSCM support.

b. Who requested the survey.

c. When the survey was accomplished and by whom.

d. Description of the support provided.

e. Findings/Observations if security vulnerabilities or hazards were discovered.

f. Recommendations that either mitigate or eliminate the security vulnerabilities.

g. Name of local person who received the out-brief.

2. Reports shall be signed by the responsible senior security official who has operational oversight of the TSCM team. Copies of TSCM reports shall be provided to the DSMD.

7.15.1.6 Discovery of a Device

Upon discovery of a suspected eavesdropping device, the following actions shall be taken:

a. The area shall be secured and placed under continuous surveillance.

b. A report, classified Secret, shall be submitted, without delay, to the DSMD. At a minimum, the report shall contain the following.

(1) Date and time of the discovery.

(2) Facility and area where found.

(3) Specific location of the suspected find.

(4) Description of suspected device (e.g., wired microphone, modified telephone, RF transmitter, etc.).

(5) Method of discovery.

(6) Name(s) and any additional information of personnel who discovered the suspected device.

(7) Best estimate as to whether any foreign intelligence service was alerted to the discovery.

b. Only the responsible official at the facility shall be notified of the discovery and the actions taken. Information of the suspected discovery shall not be released to other persons, until such release has been coordinated with and approved by the DSMD.

c. No effort shall be made to test the specific device or to attempt to remove the suspected device, until such actions have been authorized by the DSMD.

7.15.1.7 Classification Requirements

a. NASA TSCM Security Classification Guide SCG-17, dated August 1992 is hereby rescinded.

b. The following is classification requirements for NASA TSCM operations as outlined in USSPB Procedural Guide 1 and shall serve as the TSCM classification Guide for the Agency:

á

Information that Reveals	Shall be Classified
á	á
(1) Pending or current TSCM operation.	Secret
á	á
(2) Completed TSCM operation.	Confidential
á	á
(3) A request for TSCM service.	Secret
á	á
(4) Major security vulnerabilities of an area.	Secret
á	á
(5) Minor vulnerabilities.	Confidential
á	á
(6) The discovery of a device.	Secret
á	á
(7) Facility/program threat assessments as part of TSCM service.	Secret
á	á
(8) Penetration techniques.	Up to Secret
á	á

(9) TSCM equipment capabilities/limitations; budget or procurement actions; and/or policies and procedures	Up to Secret
á	á
(10) TSCM team membership, orders, or agency affiliation.	Up to Secret

2. The following shall be used for the Classified by Line, Reason, and Declassification:

Classified by: USSPB Procedural Guide 1

Reason: 1.4c

Declassify on: March 24, 2024

7.16 Dealing With Demonstrations

7.16.1. Objectives.

The primary objectives in dealing with demonstrations are to restrict demonstration activity to areas outside Centers and to preserve peace while protecting the rights of demonstrators to assemble peacefully and exercise free speech.

7.16.2. Use of Force.

7.16.2.1. Demonstrators who have illegally entered NASA property shall be politely requested to leave voluntarily.

7.16.2.2. Only the minimum amount of physical force necessary shall be used to remove demonstrators who refuse to leave NASA buildings or grounds.

7.16.2.3. Verbal abuse or verbal threats alone by a demonstrator cannot be the basis for use of physical force.

7.16.3. Law Enforcement.

7.16.3.1. The CCS for each Center shall make reasonable efforts to use non-arrest methods to manage crowds.

7.16.3.2. If demonstrators are disorderly or refuse to leave NASA buildings or grounds, then law enforcement officers who have the appropriate jurisdiction shall be summoned for support.

7.16.3.3. Ensure that sufficient law enforcement personnel are on hand and then inform the demonstrators that they must leave the NASA building or grounds within a brief period of time, such as 15 minutes, or face arrest for trespassing.

7.16.3.4. If the demonstrators still refuse to leave, law enforcement personnel shall take necessary action to effect an arrest for, at a minimum, trespassing and remove them from the building or grounds as quickly as possible.

7.16.4. Center Directors; Director, Headquarters Operations; and AA/OSPP shall make the following decisions:

7.16.4.1. When to request outside Federal, State, county, or local law enforcement personnel to enter a Center to enforce the law.

7.16.4.2. When to curtail activities or to close the gates of the Center.

7.16.4.3. When to dispatch response teams to demonstrations.

7.16.5. The CCS of each Center has the following responsibilities:

7.16.5.1. Identify the group leadership and purpose of the demonstration.

7.16.5.2. Determine the expected size, type, activity, and time of planned demonstrations.

7.16.5.3. Evaluate and dispatch information to the DSMD.

7.16.5.4. Upon instructions from the Center Director, coordinate a plan of action with local law enforcement officials.

7.16.5.5. Obtain support from the Center's Public Affairs Office (PAO), the local Office of Inspector General, the Center's Office of the Chief Counsel, and the U.S. Attorney's Office, as necessary and appropriate.

7.16.5.6. Ensure that the Statement of Work for the contract security force includes training in dealing with demonstrators as annual in-service training, and as refresher training immediately prior to a demonstration, when possible.

7.16.5.7. Ensure that all personnel who are authorized to carry firearms under the provisions of paragraph 7.9 of this Chapter and all personnel whose actions are governed by the limitations and regulations at 14 CFR Part 1203b, Arrest Authority and Use of Force receive training in dealing with demonstrators as an annual in-service training and as refresher training immediately prior to a demonstration.

7.16.5.8. Maintain an event log, commencing at the time information is first received, of a demonstration and detailing thereafter all significant events, times, places, and actions with the name of the NASA official authorizing such actions.

7.17 Threat Conditions (THREATCONS) Program

7.17.1. General.

7.17.1.1. The protection of NASA employees and assets from acts of terrorism at NASA-owned or leased property in the United States or abroad shall be given priority, especially during periods of heightened threat.

7.17.1.2. Although absolute protection against such acts is not possible, protective procedures shall be based on the threat level and reflect a balance among the degrees of protection required, the resources available, Agency mission requirements, and other pertinent factors.

7.17.1.3. In addition to assistance from the DSMD, the Center shall obtain support from local representatives such as the FBI, Department of State, NASA OIG, and state and municipal law enforcement agencies.

7.17.2. THREAT CONDITIONS (THREATCONS).

7.17.2.1. This section explains the establishment of the NASA Threat Condition (THREATCON) program designed to meet the requirements of the National Threat Warning System developed and implemented by the Department of Homeland Security (DHS).

7.17.2.2. NASA Centers hosting military organizations as tenants, residing as a tenant on a military installation, or situated contiguous to a military installation, shall establish mutually agreed upon notification systems for ensuring Department of Defense's use of ALPHA designators under the DoD Force Protection Condition (FPCON) concept vice COLOR coded designators under the DHS Threat Condition concept does not conflict with NASA's implementation of Agency Threat Conditions established under Homeland Security Presidential Directive (HSPD) 3, Homeland Security Advisory System.

7.17.2.3. The warning system ranges from NASA's basic, level 1, everyday security policy (THREATCON GREEN) through additional four graduated levels of increased security, culminating at the most stringent level (THREATCON RED).

7.17.2.4. The warning system is intended to standardize terms and establish standardized security measures that can be initiated by the AA/OSPP and Center Directors through the Agency-wide emergency notification system.

7.17.2.5. Every Government agency is required to use this Threat Condition Program that provides for a greater consistency to threat reactions at both the national and Agency-level.

7.17.2.6. The AA/OSPP shall initiate, and shall change, or rescind NASA-wide THREATCONS.

7.17.2.7. Center Directors shall implement THREATCONS initiated by the AA/OSPP and may implement higher THREATCONS for their Center based on the local threat situation. They shall not lower or rescind a THREATCON initiated by the AA/OSPP.

7.17.2.8. The DSMD shall monitor the threat status in the Agency and maintain close liaison with the Department of Homeland Security and National-level intelligence and security agencies for timely and accurate threat information.

7.17.2.9. The CCS shall maintain close liaison with the local FBI offices and local law enforcement agencies for threat information.

7.17.2.10. NASA THREATCONS and associated actions are outlined in Appendix L, NASA THREATCON Actions.

7.18 Hazardous Material Security

7.18.1. NASA programs use many different hazardous materials in meeting mission objectives. It is imperative that the use, storage, and protection of these materials be given the highest priority necessary to ensure the safety of NASA personnel and the general public.

7.18.2. In coordination with Center safety, logistics, environmental, and Transportation officials, Center Security Offices shall develop and implement security plans specifically designed to provide maximum protection in the transportation, receipt, access, use, storage, and accountability of hazardous materials used by NASA. Security Plans shall include:

a. Review of shipping/transportation procedures to ensure appropriate precautions are in place. Recommend changes/adjustments as appropriate.

b. Appropriate sharing of threat information associated wi , th the targeting of hazardous materials.

c. Establishment of Center-specific receipt, escort, and hand-off procedures, as appropriate.

d. Establishment of security procedures for permanent and temporary storage/holding areas.

| TOC | ChangeHistory | Preface | Chapter1 | Chapter2 | Chapter3 | Chapter4 | Chapter5 | Chapter6 | Chapter7 | Chapter8 | Chapter9 | Chapter10 | AppendixA | AppendixB | AppendixC | AppendixD | AppendixE | AppendixF | AppendixG | AppendixH | AppendixI | AppendixJ | AppendixK | AppendixL | AppendixM | AppendixN | AppendixO | ALL |

| NODIS Library | Organization and Administration(1000s) | Search |

DISTRIBUTION:
NODIS